KR 2003027066

DIALOG(R)File 351:Derwent WPI

0013062474
WPI ACC NO: 2003-142386/
XRPX Acc No: N2003-113082
Scalable content protection-enabled device e.g. audio/video receiver, authenticates destination device as strong/weakly protected device by verifying received certificate with certifying authority/local public key
Patent Assignee: BOUSIS L P F (BOUS-I); KONINK PHILIPS ELECTRONICS NV (PHIG)
Inventor: BOUSIS L P F
9 patents, 98 countries

Patent Family

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
EP 1271875	A1	20030102	EP 2001202382	A	20010621	200314	B
WO 2003001764	A1	20030103	WO 2002IB2415	A	20020620	200314	E
KR 2003027066	A	20030403	KR 2003702566	A	20030221	200353	E
BR 200205665	A	20030729	BR 20025665	A	20020620	200365	E
			WO 2002IB2415	A	20020620		
EP 1402701	A1	20040331	EP 2002735904	A	20020620	200424	E
			WO 2002IB2415	A	20020620		
AU 2002309194	A1	20030108	AU 2002309194	A	20020620	200460	E
US 20040187001	A1	20040923	WO 2002IB2415	A	20020620	200463	E
			US 2003480337	A	20031211		
JP 2004533194	W	20041028	WO 2002IB2415	A	20020620	200471	E
			JP 2003508037	A	20020620		
CN 1518825	A	20040804	CN 2002812382	A	20020620	200475	E

Priority Applications (no., kind, date): EP 2001202382 A 20010621

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
EP 1271875	A1	EN	20	8	
Regional Designated States,Original: AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR					
WO 2003001764	A1	EN			
National Designated States,Original: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW					
Regional Designated States,Original: AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW					
BR 200205665	A	PT			PCT Application WO 2002IB2415 Based on OPI patent WO 2003001764
EP 1402701	A1	EN			PCT Application WO 2002IB2415 Based on OPI patent WO 2003001764
Regional Designated States,Original: AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR					
AU 2002309194	A1	EN			Based on OPI patent WO 2003001764
US 20040187001	A1	EN			PCT Application WO 2002IB2415

JP 2004533194 W JA 56 PCT Application WO 2002IB2415
Based on OPI patent WO 2003001764

Alerting Abstract EP A1

NOVELTY - An authentication unit (114) of a source device (110) authenticates a destination device (130) as a strongly protected device, when a certificate for public key from the destination device is verified successfully with available public key of a certifying authority (CAPK). The destination device is authenticated as weakly protected device, when the certificate is verified successfully with locally available public key (SPK).

DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

1.Remote device authentication method; and

2.Computer program product for authenticating remote device.

USE - Scalable content protection enabled device such as audio/video receivers and players, set top boxes, general purpose computers, mobile telephones, Internet applications.

ADVANTAGE - By authenticating the devices as weakly protected and strongly protected devices, the data is transmitted securely between the devices. Hence, data transfer efficiency is enhanced.

DESCRIPTION OF DRAWINGS - The figure shows a schematic view of the scalable content protection enabled device.

110 Source device
114 Authentication unit
130 Destination device

Technology Focus

INDUSTRIAL STANDARDS - The connection between the source and destination devices is established according to IEEE 1394, 802.11, HIPERLAN or Bluetooth standards.

Original Publication Data by Authority

Original Abstracts:

A first device (110) arranged for exchanging data with a second device (130). The first device (110) receives from the second device (130) a certificate comprising a public key (UPK) for the second device. The first device (110) then authenticates the second device (130) as a strongly protected device upon a successful verification of the received certificate with a public key (CAPK) of a Certifying Authority, if the public key of the Certifying Authority is available, and authenticates the second device (130) as a weakly protected device upon a successful verification of the received certificate with a locally available public key (SPK). The second device (130) does the same to achieve mutual authentication. Having authenticated each other, the devices (110, 130) can securely set up session keys and exchange data. The data preferably has associated DRM rules.

A first device (110) arranged for exchanging data with a second device (130). The first device (110) receives from the second device (130) a certificate comprising a public key (UPK) for the second device. The first device (110) then authenticates the second device (130) as a strongly protected device upon a successful verification of the received certificate

with a public key (CAPK) of a Certifying Authority, if the public key of the Certifying Authority is available, and authenticates the second device (130) as a weakly protected device upon a successful verification of the received certificate with a locally available public key (SPK). The second device (130) does the same to achieve mutual authentication. Having authenticated each other, the devices (110, 130) can securely set up session keys and exchange data. The data preferably has associated DRM rules.

A first device (**110**) arranged for exchanging data with a second device (**130**). The first device (**110**) receives from the second device (**130**) a certificate comprising a public key (UPK) for the second device. The first device (**110**) then authenticates the second device (**130**) as a strongly protected device upon a successful verification of the received certificate with a public key (CAPK) of a Certifying Authority, if the public key of the Certifying Authority is available, and authenticates the second device (**130**) as a weakly protected device upon a successful verification of the received certificate with a locally available public key (SPK). The second device (**130**) does the same to achieve mutual authentication. Having authenticated each other, the devices (**110, 130**) can securely set up session keys and exchange data. The data preferably has associated DRM rules.

A first device (110) arranged for exchanging data with a second device (130). The first device (110) receives from the second device (130) a certificate comprising a public key (UPK) for the second device. The first device (110) then authenticates the second device (130) as a strongly protected device upon a successful verification of the received certificate with a public key (CAPK) of a Certifying Authority, if the public key of the Certifying Authority is available, and authenticates the second device (130) as a weakly protected device upon a successful verification of the received certificate with a locally available public key (SPK). The second device (130) does the same to achieve mutual authentication. Having authenticated each other, the devices (110, 130) can securely set up session keys and exchange data. The data preferably has associated DRM rules.

Selon l'invention, un premier dispositif (110) est concu pour echanger des donnees avec un deuxieme dispositif (130). Le premier dispositif (110) recoit du deuxieme dispositif (130) un certificat contenant une cle publique (UPK) destinee au deuxieme dispositif. Le premier dispositif (110) authentifie alors le deuxieme dispositif (130) en tant que dispositif fortement protege en cas de verification reussie du certificat recu contenant une cle publique (CAPK) d'un organisme de certification (si la cle publique de l'organisme de certification est disponible), et authentifie le deuxieme dispositif (130) en tant que dispositif faiblement protege en cas de verification reussie du certificat recu contenant une cle publique locale (SPK). Le deuxieme dispositif (130) effectue les memes operations afin de realiser une authentification mutuelle. Lorsque lesdits dispositifs (110, 130) ont realise l'authentification mutuelle, ces derniers peuvent creer des cles de session de maniere securisee et echanger des donnees. Lesdites donnees comportent de preference des regles DRM.
Basic Derwent Week: 200314